Description de l'offre
pour
AMP, Threat Grid, CTA, CDO, Umbrella et Cloudlock

APERÇU

Cette description de l'offre décrit les services de sécurité en nuage suivants :

- Protection avancée contre les logiciels malveillants de Cisco
- Grille Threat Grid de protection avancée Cisco contre les attaques des programmes malveillants
- Solution Cisco d'analyse cognitive des menaces (CTA)
- Démonstration de Cisco Defense Orchestrator (CDO)
- Cisco Umbrella
- Cisco Cloudlock

Le Contrat universel de nuage de Cisco (**« Contrat »**) et les modalités décrites dans le présent document régissent votre utilisation de chaque service en nuage référencé dans le présent document. Un exemplaire actualisé du contrat se trouve à : http://www.cisco.com/c/en/us/about/legal/cloud-and-software.html.

À moins d'être définis dans le texte ci-présent, les mots en lettres majuscules utilisés dans cette description d'offres sont définis à **l'annexe A**, à **l'annexe B** (pour Cloudlock) ou au contrat.

Si un service en nuage indiqué dans cette Description de l'offre est compatible avec d'autres produits Cisco ou offres de services non référencés dans le présent, ces autres produits ou solutions peuvent avoir des contrats de licence supplémentaires qui s'appliquent à votre utilisation de ces produits et les offres. Vous êtes également tenus de respecter les conditions des autres produits et offres, le cas échéant. Les modalités déterminées dans ce document s'appliquent aux services en nuage répertoriés dans cette description de l'offre qu'ils soient achetés pour une utilisation sur une base autonome, ou achetés pour être utilisés avec ces autres produits ou offres de Cisco.

CONDITIONS GÉNÉRALES

Les conditions générales suivantes s'appliquent à *tous* les services en nuage mentionnés dans la description de cette offre :

R. Assistance technique. Cisco vous fournira des services d'assistance d'abonnement aux logiciels de Cisco pour chaque service en nuage, les modalités actuelles étant situées à : http://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Software_Subscription_Support.pdf. Toutefois, les conditions de l'assistance pour les services Cloudlock et les services infonuagiques Umbrella Cloud sont décrites ci-dessous.

B. Période de maintenance programmée. Cisco réalise périodiquement des opérations de maintenance programmées visant à mettre à jour les serveurs et les logiciels utilisés pour la prestation des Services infonuagiques. Cisco accepte de faire tous les efforts raisonnables pour

vous fournir des avis préalables à toutes les périodes de maintenance planifiées ou avant toutes les interruptions planifiées qui auront des incidences sur votre utilisation du service en nuage. Nonobstant ce qui précède, le Client accepte que Cisco puisse dans certaines situations être dans l'obligation d'exécuter sans préavis diverses opérations urgentes de maintenance.

C. Renseignements de Cisco sur les menaces. Si votre utilisation du service en nuage requiert ou vous autorise à utiliser les renseignements de Cisco sur les menaces, vous (et vos agents agissant en votre nom) ne pouvez utiliser de tels renseignements de Cisco sur les menaces que pour votre propre usage d'un tel service en nuage et à ces produits de fournisseurs tiers ou offres de services que Cisco a défini comme étant compatible. Vous acceptez de ne pas diffuser les renseignements de Cisco sur les menaces à des tiers.

D. Restrictions d'utilisation. Vous ne pouvez pas déployer ou utiliser un service en nuage de telle sorte qu'elle (i) dépasse la durée de la période d'abonnement applicable (p. ex., 1, 3 ou 5 ans), (ii) dépasse une limite d'utilisation ou un autre paramètre relatifs à votre licence (p. ex., nombre de Postes, Points terminaux, nombre maximal de demandes d'information, limites du nombre de périphériques, nombre de sites, le nombre de points d'accès, nombre d'utilisateurs, nombre d'hôtes, d'envois de fichiers, d'analyses, ressources, etc.) définie dans cette description d'offre, une commande, l'UGS, l'identifiant (PID) de produit ou la documentation pour le service en nuage correspondant.

E. Utilisation des logiciels. Si le service en nuage que vous utilisez comporte les analyses des programmes malveillants et de fichiers exécutables sur les systèmes d'exploitation ou applications de Microsoft ou d'autres fournisseurs tiers, vous êtes alors tenu d'obtenir et de respecter ces licences d'utilisation de produits de Microsoft ou de fournisseurs tiers pour chaque appareil d'utilisateur final fonctionnant avec de tels produits de Microsoft et de fournisseurs tiers.

F. Utilisation des données par Cisco. Dans le cadre de votre utilisation des services en nuage, vous produirez et rendrez accessible à Cisco ou générerez par votre utilisation du ou des services en nuage (i) des données client, (ii) des données réseau et (iii) des métadonnées Cisco Cloudlock (si vous utilisez Cisco Cloudlock) tous ces éléments seront collectivement désignés ci-après (de « **Données** »). Vous reconnaissez et consentez à ce que Cisco puisse utiliser les données aux fins (a) de fournir, améliorer, maintenir, personnaliser ou prendre en charge les services en nuage; et (b) de création de données statistiques. Cisco est autorisée à transmettre des Données (x) au sein de Cisco et de ses filiales internationales ainsi qu'avec nos fournisseurs agréés, et ce, uniquement aux fins autorisées ci-dessus; (y) afin de se conformer à la Loi et en vertu de la politique de Cisco relative aux demandes des services policiers à http://www.cisco.com/c/en/us/about/trust-transparency-center/validation/report.html; ou (z) avec votre consentement écrit. Tous les renseignements personnels compris dans les Données sont définis et assujettis aux conditions définies au contrat.

Certaines Données que Cisco recueille du service en nuage, ou que vous transmettez ou rendez accessibles à Cisco dans le cadre de votre utilisation du service en nuage, sont nécessaires pour les utilisations essentielles et la fonctionnalité dudit service en nuage. Les Données sont également utilisées par Cisco pour fournir des services connexes comme l'assistance technique et pour améliorer de façon continue l'exploitation, l'efficacité de la sécurité et des fonctionnalités des services en nuage. Pour ces raisons, votre seul choix pour refuser la collecte de Données sera de désinstaller ou de désactiver le service en nuage correspondant. Vous pourriez cependant, être en mesure de configurer le service en nuage pour restreindre certaines des Données qui peuvent être collectées, comme décrit dans les documents correspondants. Certains services en nuage permettent de modifier les Données en fonction de vos configurations souhaitées (p. ex., en imposant une règle pour configurer les données accessibles par le public à un paramétrage privé).

Consultez les documents pertinents pour plus d'informations sur la manière dont vous pouvez configurer la collecte des Données.

G. Utilisation des Données statistiques. Vous cédez à Cisco par la présente une licence non exclusive, transférable, irrévocable, mondiale, perpétuelle, libre de droits et intégralement acquittée pour l'utilisation des Données statistiques quel qu'en soit l'usage, y compris, aux fins d'amélioration, de mise au point, de mise en marché ou de promotion des produits et services Cisco incluant les services en nuage.

H. Sécurité des Données. Cisco mettra à jour des mécanismes de protection administratifs, physiques et techniques conformes aux normes de l'industrie et à la Documentation, conçues pour assurer la sécurité, la confidentialité et l'intégrité des Données utilisées par Cisco.

I. Garanties. Outre les garanties et les clauses de non responsabilité es avis prévues au contrat, Cisco garantit qu'elle offrira les services en nuage selon les normes générales du domaine raisonnablement applicables à la présente disposition. CISCO NE FAIT AUCUNE REPRÉSENTATION OU GARANTIE VOULANT QUE LES SERVICES EN NUAGE GARANTISSENT LA SÉCURITÉ ABSOLUE EN RAISON DU DÉVELOPPEMENT CONTINUEL DE NOUVELLES TECHNIQUES POUR S'INTRODUIRE DANS LES FICHIERS, LES RÉSEAUX ET LES POINTS TERMINAUX. CISCO NE FAIT AUCUNE REPRÉSENTATION VOULANT QUE LES SERVICES EN NUAGE PROTÈGENT TOUS VOS FICHIERS, RÉSEAUX, OU POINTS TERMINAUX CONTRE TOUS LES PROGRAMMES MALVEILLANTS, VIRUS OU ATTAQUES MALVEILLANTES DE TIERS. CISCO NE FAIT AUCUNE REPRÉSENTATION OU GARANTIE RELATIVE AUX SYSTÈMES OU SERVICES DE FOURNISSEURS TIERS AUXQUELS UN SERVICE EN NUAGE S'INTÈGRE OU CONCERNANT UNE ASSISTANCE PERMANENTE POUR L'INTÉGRATION. LES INTÉGRATIONS MISES À VOTRE DISPOSITION NE SONT PAS GÉNÉRALEMENT DES PRODUITS MIS EN MARCHÉ INCLUS DANS VOTRE COMMANDE SONT FOURNIS « TELS QUELS ».

DESCRIPTIONS D'OFFRE ET CONDITIONS SUPPLÉMENTAIRES

Les services en nuage ainsi que les conditions générales supplémentaires qui s'appliquent à chaque service en nuage éventuel sont décrits ci-dessous. Si vous n'avez pas acheté un abonnement ou une licence pour utiliser des services en nuage énumérés ci-dessous, alors la description et les conditions supplémentaires ci-après pour un tel service en nuage ne s'appliquent pas dans votre cas.

Protection avancée contre les programmes malveillants (« AMP »)

Description. AMP est une solution infonuagique d'analyse et de protection avancées contre les programmes malveillants qui vous permet de mener des analyses de métadonnées des Fichiers dans le but de détecter les menaces de programmes malveillants et d'attaques informatiques. Des hachages cryptographiques des fichiers sont collectés et communiqués à un serveur Cisco de gestion en nuage où des analyses de la réputation de Fichier sont exécutées et un classement est fait pour déterminer si le Fichier est inoffensif, malveillant ou inconnu. Si un classement ne peut être effectué après analyse de hachage d'un fichier, vous avez l'option (selon les licences achetées) de soumettre le fichier à AMP Threat Grid (décrite ci-dessous) pour une des analyses plus poussées en bac de sable jusqu'à la limite quotidienne autorisée de demandes. Après analyse

du fichier, AMP interviendra en fonction du classement (p. ex., en supprimant le fichier et en le mettant en quarantaine si ce dernier est jugé être de nature malveillante). AMP est offert dans divers formats dont AMP pour les points terminaux, AMP pour la messagerie courriel, AMP pour le Web, AMP sur NGIPS (AMP pour réseaux), AMP sur NGFW et AMP pour Meraki MX. Consultez la documentation d'AMP pour plus d'informations sur ses caractéristiques techniques, ses exigences en matière de configuration, ses fonctionnalités et autres caractéristiques.

AMP Threat Grid

Description. La grille de protection avancée Threat Grid est une solution infonuagique de veille de renseignements et d'analyse en bac à sable sur les menaces et les programmes malveillants où vous pouvez soumettre des échantillons de maliciels pour une analyse plus poussée. La grille de protection avancée AMP Threat Grid analyse chaque fichier afin d'enregistrer son comportement et déterminer s'il est malveillant. La grille de protection avancée AMP Threat Grid recherche et mettra en corrélation des éléments de données d'un échantillon de programme malveillant avec des millions d'échantillons collectés et provenant de partout dans le monde pour vous donner un aperçu global des attaques de programmes malveillants et de ses associations. Consultez la documentation de Cisco AMP Threat Grid pour obtenir de plus amples renseignements sur ses caractéristiques techniques, ses exigences en matière de configuration, ses fonctionnalités et autres caractéristiques.

Conditions supplémentaires.

Soumissions de fichier. Lorsque vous envoyez un fichier au nuage AMP Threat Grid, il est possible qu'en raison de la fonctionnalité d'analyse comparative fournie avec AMP Threat Grid qu'un autre utilisateur puisse examiner et déterminer le contenu d'un tel Fichier, car Cisco AMP Threat Grid fait appel à sa communauté d'utilisateurs pour contrer les programmes malveillants. Si vous choisissez de soumettre un fichier à AMP Threat Grid comme Fichier Privé, ce fichier sera alors inaccessible pour l'analyse par d'autres utilisateurs. Si vous n'indiquez pas que le fichier est en format Privé à la soumission au nuage de la grille de protection avancée d'AMP, un tel Fichier est un fichier non confidentiel qui peut être inspecté par d'autres utilisateurs de Cisco AMP Threat Grid et ne sera pas jugé comme une information confidentielle. Les autres utilisateurs de Cisco AMP Threat Grid ont accès aux fichiers non confidentiels et ont donc la capacité de consulter le contenu des fichiers non confidentiels. La capacité de présenter un fichier à AMP Threat Grid comme fichier privé peut nécessiter des licences supplémentaires ou des abonnements.

Si un fichier comprend des informations critiques ou renseignements confidentiels que vous ne voulez pas que d'autres utilisateurs de Cisco AMP Threat Grid ont la capacité à analyser, vous devrez (i) vous abstenir de soumettre le fichier à AMP Threat Grid ou (ii) soumettre le fichier en format Privé, (iii) soumettre le fichier à une version locale du dispositif Cisco AMP Threat Grid pour une confidentialité maximale. Concernant les fichiers non confidentiels que Cisco recueille de votre utilisation de la solution AMP Threat Grid, vous cédez à Cisco et à ses fournisseurs de services agréés une licence non exclusive, perpétuelle, irrévocable, transférable, mondiale, libre de droits et entièrement acquittée, incluant le droit d'octroyer des sous-licences, d'utiliser tous les fichiers non confidentiels pour vous offrir la solution AMP Threat Grid ainsi qu'à d'autres utilisateurs et pour toute autre fin.

Analytique cognitive des menaces (« CTA »)

Description. CTA est une solution infonuagique d'analyse comportementale de programmes malveillants qui se sert des journaux de mandataires Web des solutions d'accès Web de Cisco

comme le dispositif de sécurité Web Cisco Web Security Appliance (« WSA ») et la sécurité Web en nuage (« CWS ») ou toutes les autres plateformes de fournisseurs tiers ou NetFlow pris en charge par Cisco Stealthwatch pour détecter les programmes malveillants présents dans votre environnement et rechercher les activités malveillantes actives connexes. CTA est accessible dans le cadre de la protection AMP avancée des points terminaux et du Web sur les licences des appareils WSA ou en tant que licence autonome ou ajoutée à d'autres produits pris en charge, le cas échéant. Consultez la documentation de CTA pour obtenir de plus amples renseignements sur ses caractéristiques techniques, ses exigences en matière de configuration, ses fonctionnalités et ses autres caractéristiques.

Conditions supplémentaires.

Soumissions au journal des mandataires et à NetFlow. Pour utiliser CTA, vous devez soumettre les journaux des mandataires Web à partir d'une plateforme prise en charge ou sur NetFlow de Cisco Stealthwatch comme décrit dans la documentation. Ces journaux peuvent comporter des données identifiables telles que le nom d'utilisateur, le nom de l'appareil, l'adresse IP et les informations de navigation. CTA peut utiliser ces données pour effectuer une analyse pour déterminer la présence de programmes malveillants sur vos systèmes et associer des communications entrant ou sortant de ces systèmes touchés à des ordinateurs ou des sites malveillants suspects. Si vous ne souhaitez pas transmettre vos journaux de mandataire Web ou NetFlow et les renseignements relatifs au nuage de CTA pour être en mesure d'analyser les programmes malveillants actifs à l'intérieur de votre environnement, vous ne devez pas activer CTA.

Cisco Defense Orchestrator (« CDO »)

Description. CDO est une application infonuagique de gestion des règles de sécurité qui permet à l'utilisateur de gérer plusieurs produits de sécurité Cisco grâce aux fonctionnalités suivantes : gestion des changements de règles, analyse et optimisation des règles, contrôles et rapports sur les règles et orchestration des changements de règles. Consultez la documentation sur la solution CDO pour obtenir de plus amples renseignements sur ses caractéristiques techniques, ses exigences en matière de configuration, ses fonctionnalités et autres caractéristiques.

Cisco Umbrella

Description. La solution Cisco Umbrella est une plateforme infonuagique de sécurité de la couche DNS (système de noms de domaine) qui offre la première ligne de défense contre les menaces sur Internet en bloquant les demandes de destinations malveillantes (les domaines, les adresses IP, les URL) avant que la connexion soit établie. Il fournit une protection contre les menaces sur tous les ports et protocoles et peut protéger l'accès Internet à tous les appareils sur votre réseau, tous les sites et les utilisateurs en déplacement. Cisco Umbrella étude permet d'accéder à certains contenus de Cisco Threat sur les domaines malveillants, IPS, réseaux et condensés de fichier. En se servant d'un ensemble varié de données tiré de milliards de demandes quotidiennes DNS et de vues en direct des connexions entre différents réseaux sur Internet, la solution d'enquête Cisco Umbrella Investigate applique des modèles statistiques et des renseignements recueillis par des spécialistes pour repérer les infrastructures des attaquants. Les données générées par Cisco Umbrella Investigate peuvent être consultées à partir d'une console Web ou d'une API. Cisco Umbrella comprend différentes options de licence pour les réseaux cellulaires, les réseaux en succursale, les réseaux professionnels, les analyses, les plateformes, les enquêtes et les réseaux étendus WLAN. Consultez la documentation Cisco Umbrella pour obtenir de plus amples

renseignements sur ses caractéristiques techniques, ses exigences en matière de configuration, ses fonctionnalités et autres caractéristiques.

Conditions supplémentaires.

Attribution des licences. Les postes ne peuvent être affectés à l'utilisation de plus d'un utilisateur, mais peuvent être réattribués à de nouveaux employés/sous-traitants qui remplacent les anciens utilisateurs autorisés ayant quitté leur poste ou dont les fonctions ont changé et qui n'utilisent plus Cisco Umbrella.

Engagement d'accessibilité au service. Cisco déploiera tous les efforts commercialement raisonnables pour maintenir un taux d'accessibilité à Cisco Umbrella de 99,999 % de chaque mois du calendrier. L'accessibilité sera calculée en divisant le total des minutes où la plateforme est accessible durant un mois de calendrier correspondant par le nombre total de minutes de ce même mois, moins les minutes où Cisco Umbrella est inaccessible en raison des périodes de maintenance planifiées et imputables aux interventions de tiers (définies ci-dessous), le tout multiplié par 100. La formule du calcul est comme suit :

$$\text{Accessibilité} = (X \div Y) \times 100$$

X = total des minutes d'accessibilité au cours du mois de calendrier

Y= (total des minutes dans ce même mois de calendrier x) - (total des minutes d'inaccessibilité en raison des périodes de maintenance planifiées et des interventions de tiers)

Aux fins de ce calcul, (**i) une « Inaccessibilité »** signifie que Cisco Umbrella est totalement inaccessible même si votre connexion Internet fonctionne correctement, (ii) « **Temps d'accessibilité** » désigne le nombre de minutes où Cisco Umbrella était accessible, à l'exception des périodes d'inaccessibilité pour des opérations de maintenance planifiées et des interventions de tiers, et (iii) une **« Intervention d'un tiers** » désigne toute intervention hors de la volonté de Cisco y compris, l'efficacité des réseaux Internet ou de carrefours d'échanges de données qui sont gérés par d'autres entreprises, les conflits de travail, les pénuries, les émeutes, les insurrections, les incendies, les inondations, les perturbations météorologiques ou solaires, les explosions, les événements de force majeure, les conflits armés, les actes de terrorisme, les interventions gouvernementales, les conditions de travail, les séismes et les pénuries. En cas de différend, Cisco rendra sa décision en toute bonne foi sur la base de ses journaux du système, des rapports de surveillance et des registres de configuration et en ce qui concerne la préséance des relevés ceux de Cisco prévalent sur ceux des clients. Cisco ne peut être tenue responsable en aucun cas des interruptions de Cisco Umbrella causées par des interventions de tiers.

Période de maintenance planifiée de Cisco Umbrella Dans tous les cas où la période de maintenance planifiée pour Cisco Umbrella sera effectuée, Cisco fera tout en son pouvoir raisonnable pour s'assurer que cette période de maintenance planifiée relative à l'accessibilité de Cisco Umbrella pour plus de trente (30) minutes soit effectuée entre minuit et 5 h (heure du Pacifique), du lundi au vendredi (excluant les jours fériés aux États-Unis), ou entre midi et 5 h du matin (heure du Pacifique) le samedi, dimanche et les jours fériés aux États-Unis.

Descriptions des niveaux d'assistance technique. L'assistance technique pour Cisco Umbrella est assurée en vertu du niveau d'assistance technique applicable et des priorités ou réponses cibles définies ci-dessous :

Niveau de l'assistance technique	Description
Niveau de base	• Accès seulement par courriel • Accès aux outils en ligne (p. ex., les bases de connaissances, les forums, la Documentation, les portails de cas et les notifications)
Or	• Accès par courriel • Accès aux outils en ligne (p. ex., les bases de connaissances, les forums, la Documentation, les portails de cas et les notifications) • Assistance téléphonique 24 h sur 24, 7 jours sur 7 pour les demandes de niveau prioritaire P1 • Assistance téléphonique 24 h pour les demandes de niveaux prioritaires P2 et P3 (dimanche à 16 h (HNP) au vendredi 17 h (HNP).
Platine	• Gestionnaire de compte technique (TAM) dédié • Accès par courriel • Accès aux outils en ligne (p. ex., les bases de connaissances, les forums, la Documentation, les portails de cas et les notifications) • Assistance téléphonique 24 h pour les demandes de niveau prioritaire P1 • Assistance téléphonique 24 h pour les demandes de niveaux prioritaires P2 et P3 (dimanche à 16 h (HNP) au vendredi 17 h (HNP).

Niveaux de priorité et de réponse.

Priorité d'assistance	Délai d'intervention cible	Description
P1 Inaccessibilité (telle que définie ci-dessus)	--30 minutes pour les demandes de téléphone --2 heures pour les demandes de courriel	Cisco travaillera pour la résolution concernant une base 24 h sur 24 et 7 jours sur 7 ou pour résoudre le problème, ou développer un contournement raisonnable.
P2 : Problème technique	1 jour ouvrable	Un problème survient lorsque Cisco Umbrella est accessible, mais que les délais de traitement sont lents alors que votre connexion Internet fonctionne correctement. Les problèmes incluent des questions techniques ou des problèmes de configuration relatifs aux comptes client qui ont des effets modérés sur votre capacité d'utiliser Cisco Umbrella. Cisco travaillera pour la résolution continuellement pendant les heures d'ouverture jusqu'à ce que le problème ait été résolu, ou qu'un plan a été élaboré et convenu entre vous et Cisco.

Priorité d'assistance	Délai d'intervention cible	Description
P3 : Demande de renseignements	2 jours ouvrables	Les demandes d'information comprennent les questions relatives au compte, les réinitialisations de mot de passe et les questions de fonctionnalité. Le personnel de Cisco sera affecté à la résolution du problème au moment de la réponse ou dès que possible par la suite.

Cisco Cloudlock

Description. Cisco Cloudlock est un courtier de sécurité en nuage de l'accès du nuage (CASB) et une plateforme de cybersécurité de nuage qui aide les organisations sécurisées pour tirer le meilleur des applications dans le nuage. CISCO CloudLock offre une visibilité et un contrôle pour les environnements en logiciels-service (« SaaS » en plateformes-services (« PaaS ») et infrastructures-service (« IaaS ») pour les utilisateurs, les données et les applications. La fonctionnalité essentielle de Cisco Cloudlock couvre les trois cas d'utilisation suivants :

- Prévention des pertes de données (« **DLP** ») : Cisco Cloudlock offre la fonctionnalité de DLP qui surveille des environnements infonuagiques pour détecter et sécuriser les informations confidentielles au moyen de règles prêtes à l'emploi ainsi que des règles adaptées et modulaires. Les interventions automatisées peuvent réduire les risques d'y remédier en cas de notifications de violations de règle, y compris les avis envoyés à l'utilisateur final, le cryptage au niveau des fichiers, a migration de responsabilité et les quarantaines.

- Analyse du comportement de l'utilisateur et de l'entité (**« UEBA** ») : Cisco Cloudlock offre une fonctionnalité UEBA sur toutes les plateformes pour les environnements SaaS, IaaS, PaaS et d'identité-service **(**« IDaaS »). Cisco Cloudlock tire profit des algorithmes d'apprentissage automatique avancés pour détecter les anomalies basées sur des facteurs tels que les activités hors des pays figurant sur la liste blanche et les actions à distance.

- Pare-feu d'applications (« **Applications** ») : Les applications de Cisco Cloudlock détectent les applications en nuage connectées à votre environnement d'entreprise, et communique une notation participative de confiance de la communauté pour les applications individuelles, ainsi que la capacité d'interdire ou de mettre sur une liste blanche en fonction du profil de risque et de l'étendue des accès, la sensibilisation des employés par des alertes par courriel et le retrait du droit d'utilisation des applications par lots dans toute la base de clients.

CISCO CloudLock offre des solutions intelligentes de cybersécurité pratiques grâce à son CyberLab dirigé par des scientifiques et à des analyses de sécurité participatives. Le CyberLab fournit des analyses pour détecter, rechercher et analyser, tout en informant les clients et d'autres parties des tendances en matière de sécurité, et des menaces. Consultez la documentation de Cloudlock pour obtenir de plus amples renseignements sur ses caractéristiques techniques, ses fonctionnalités et autres caractéristiques.

Conditions supplémentaires.

Définitions. Les définitions relatives à Cloudlock sont décrites à **l'annexe B.**

Engagement d'accessibilité au service. Cisco déploiera tous les efforts commerciaux raisonnables pour maintenir un taux d'accessibilité à Cisco Cloudlock de 99,9 % tous les mois du calendrier. L'accessibilité sera calculée en divisant le nombre total de minutes d'accessibilité (définie ci-dessous) durant le mois de calendrier correspondant par le nombre total de minutes dans ce même mois, moins les minutes d'inaccessibilité de Cisco Cloudlock (définies ci-dessous) en raison de la période de maintenance planifiée et imputable aux interventions de tiers (définies ci-dessous), le tout multiplié par 100. La formule du calcul est comme suit :

$$\text{Accessibilité} = (X \div Y) \times 100$$

X = total des minutes d'accessibilité au cours du mois de calendrier

Y= (total des minutes dans ce même mois de calendrier) - (total des minutes d'inaccessibilité en raison des périodes de maintenance planifiées et des interventions de tiers)

Aux fins de ce calcul, (**i) l'« Inaccessibilité »** désigne le fait que Cisco Cloudlock est totalement inaccessible quand votre connexion Internet fonctionne correctement, (ii) « **Accessibilité** » désigne le nombre de minutes où il n'y a eu aucune défaillance de Cisco Cloudlock, à l'exception des interruptions pour des opérations de période de maintenance planifiée et de tiers, et (iii) une **« Intervention de tiers** » désigne toute intervention hors de la volonté de Cisco y compris, l'efficacité des réseaux Internet ou des carrefours d'échanges de données qui sont gérés par d'autres entreprises, les conflits de travail, les pénuries, les émeutes, les insurrections, les incendies, les inondations, les perturbations météorologiques ou solaires, les explosions, les événements de force majeure, les conflits armés, les actes de terrorisme, les interventions gouvernementales, les conditions de travail, les séismes et les pénuries. En cas de différend, Cisco rendra sa décision en toute bonne foi sur la base de ses journaux du système, des rapports de surveillance et des registres de configuration et en ce qui concerne la préséance des relevés ceux de Cisco prévalent sur ceux des clients. Cisco ne peut être tenue responsable d'aucune défaillance de Cisco Cloudlock provenant des actions de tiers.

Maintenance planifiée. Dans tous les cas où la période de maintenance planifiée pour Cisco Cloudlock sera effectuée, Cisco effectuera des tentatives raisonnables pour faire en sorte que cette période de maintenance planifiée qui influe sur l'accessibilité de Cisco Cloudlock pour plus de trente (30 minutes) soit effectuée entre minuit et 5 h du matin (heure de l'Est), du lundi au vendredi (excluant les jours fériés aux États-Unis), ou entre l'heure de l'Est de 12 h et 5 h du matin (heure de l'Est) le samedi, le dimanche et les jours fériés aux États-Unis.

Restrictions d'utilisation. Les limites suivantes s'appliquent à votre utilisation de Cisco Cloudlock :

Indicateur	**Limite** L
Nombre d'utilisateurs	Abonnement limité à la quantité applicable d'utilisateurs déterminés à la commande.

Indicateur	Limite L
Nombre de domaines couverts de services en nuage	À moins que la commande ne le précise autrement, votre abonnement est limité à un domaine unique pour chacun des services en nuage couverts.
Nombre de règles en vigueur	Jusqu'à 30
Restrictions relatives aux licences professionnelles API	Jusqu'à 100 demandes relatives aux licences professionnelles API par licence d'utilisateur pour les services de base Cloudlock par jour (mesurées globalement : 100 x nombre d'utilisateurs pour les services de base de Cisco Cloudlock couvertes par l'abonnement), mais sans dépasser 10 000 demandes relatives à une licence professionnelle API par jour, globalement. Une demande relative à une licence professionnelle API est une demande auprès de Cisco Cloudlock effectuée sur un système externe. Cette limite ne s'applique pas aux appels API entre Cisco Cloudlock et le service en nuage couvert.
Analyses rétroactives de surveillance	Jusqu'à une analyse rétroactive de surveillance par mois, à l'exception des licences d'étudiant. Pour les licences d'étudiants, vous êtes limités à une analyse rétroactive de surveillance par an.
Nombre de ressources de données	Jusqu'à 1 000 ressources de données par licence utilisateur pour les services de base de Cisco Cloudlock (quantifiés globalement : 1000 x le nombre d'utilisateurs pour les services de base de Cisco Cloudlock couverts par l'abonnement).
Environnement d'essai et de mise au point	À moins que la commande ne le précise autrement, chaque abonnement de Cisco Cloudlock comprend un environnement d'essai et de mise au point.

Sécurité. Cisco Cloudlock mène un audit annuel de sécurité de type II ou de catégorie supérieure et ne réduira pas significativement les mécanismes de protection administratifs, physiques et techniques examinés relatifs à une telle vérification. Cisco mettra à jour des mécanismes de protection administratives, physiques et techniques conformes aux normes de l'industrie et à la documentation, conçues pour offrir la sécurité, la confidentialité et l'intégrité des Données client utilisées par Cisco.

Utilisation de Cloudlock des Données client. Cisco peut avoir un accès d'utilisateur afin d'afficher l'interface utilisateur de Cisco Cloudlock et de fournir une assistance technique et d'améliorer continuellement les opérations, l'efficacité de la sécurité et les fonctionnalités de Cisco Cloudlock. En outre, l'utilisation de Cisco Cloudlock nécessite des analyses automatisées des Données client

dans le cadre de sa fonctionnalité; vous reconnaissez et consentez à ces analyses des Données client dans le cadre de l'utilisation de Cisco Cloudlock.

Stockage des données. Sauf pour les métadonnées de Cisco Cloudlock, vous conservez la maîtrise des Données client et êtes responsable de sauvegarder les Données client. **Cisco Cloudlock ne conservera aucune donnée client sauf si elle constitue des métadonnées de Cisco Cloudlock.**

Les API : Les API fournies ou rendues accessibles par Cisco dans le cadre de Cisco Cloudlock sont susceptibles d'être modifiées et vous assumez les risques associés à l'utilisation des interfaces API à des fins de mise au point lorsque vous décidez de le faire. Toutes ces API sont offertes TELLES QUELLES.

Descriptions des niveaux d'assistance technique. L'assistance technique de Cisco Cloudlock est assurée selon les cibles suivantes de niveau d'assistance technique et priorités et délai de traitement cibles :

Niveau de l'assistance technique	Description
Niveau de base	• Accès seulement par courriel • Accès aux outils en ligne (p. ex., les bases de connaissances, les forums, la Documentation, les portails de cas et les notifications)
Or	• Accès par courriel • Accès aux outils en ligne (p. ex., les bases de connaissances, les forums, la Documentation, les portails de cas et les notifications) • Assistance téléphonique 24 h sur 24, 7 jours sur 7 pour les demandes de niveau prioritaire P1 • Assistance téléphonique 24 h sur 24, 7 jours sur 7 pour les demandes de niveaux prioritaires P2 et P3 (dimanche à 16 h (HNP) au vendredi à 17 h (HNP).

Niveaux de priorité et de réponse.

Priorité d'assistance	Délai de traitement cible	Description
P1 Inaccessibilité (telle que définie ci-dessus)	--30 minutes pour les demandes d'assistance par téléphone (Or); --2 heures pour l'assistance de base	Cisco travaillera pour la résolution du problème sur une base 24 h sur 24 et 7 jours sur 7 pour résoudre le problème ou développer une solution raisonnable.

Priorité d'assistance	Délai de traitement cible	Description
P2 : Problème technique	1 jour ouvrable	Un problème survient lorsque Cisco Cloudlock est accessible, mais les délais de traitement sont lents alors que votre connexion Internet fonctionne correctement. Les problèmes peuvent être des questions techniques ou des problèmes de configuration relatifs aux comptes client qui a des effets modérés sur votre capacité à utiliser Cisco Cloudlock. Cisco travaillera en permanence sur la résolution du problème pendant les heures ouvrables jusqu'à ce que le problème ait été résolu, ou qu'un plan ait été élaboré et convenu entre vous et Cisco.
P3 : Demande de renseignements	2 jours ouvrables	Les demandes de renseignements comprennent des questions portant sur le compte, les réinitialisations de mot de passe et les questions de fonctionnalité. Le personnel de Cisco sera attribué pour travailler sur la résolution au moment de la réponse ou dès que possible par la suite.

[Les annexes suivent]

Annexe A

Glossaire

Les « renseignements de Cisco sur les menaces » désignent tous les renseignements, les contenus ou les données sur les menaces transmises par Cisco, y compris, les règles, les signatures, les flux de données relatifs aux menaces ou les flux de données d'URL et d'adresses IP suspectes pouvant être utilisés sur n'importe quel produit Cisco ou service.

La « **Documentation** » désigne les instructions d'utilisation de Cisco, les guides techniques et la documentation destinés aux utilisateurs sous forme imprimée ou dans un formulaire exploitable par machine qui décrit la fonctionnalité du service en nuage applicable ou du logiciel.

Un « **Point terminal** » désigne tout appareil capable de traiter des données qui peut accéder à un réseau, y compris des ordinateurs personnels, des appareils portables et des postes de travail de réseau.

Les « **Fichiers** » désignent les types de fichiers identifiés dans la Documentation pertinente, tel qu'un fichier d'exécution, un format de document portable PDF (PDF), des documents Microsoft Office (MS Word, MS Excel, Ms PowerPoint), et des fichiers dans un format compressé (.ZIP).

Les « **Données réseau** » désignent les données de télémétrie (comme défini dans le Contrat), et les autres données et renseignements connexes techniques concernant votre réseau informatique générés dans le cadre de votre utilisation du service en nuage y compris, le type et la version du système d'exploitation; les métadonnées et identifiants de fichiers comme les valeurs SHA-256; les données du système hôte du réseau; l'origine et la nature des programmes malveillants; les GUID des points terminaux (identifiants internationaux uniques); les adresses de protocole Internet (IP); les adresses MAC; les fichiers journaux; les journaux de mandataire Web; les fichiers de configuration; les configurations réseau; stratégies de sécurité du réseau; les types de logiciels et les applications installés sur un réseau ou un point terminal; les informations liées à l'utilisation, à l'origine de l'utilisation, aux structures de trafic et au comportement des utilisateurs d'un réseau; et les données agrégées, démographiques ou relatives au trafic réseau comme les témoins, les journaux Web, les balises Web invisibles et d'autres applications similaires.

Les « **Fichiers non confidentiels** » désignent un ou des fichiers soumis à la solution AMP Threat Grid que vous choisissez de ne pas classer comme « privé » et sont donc visibles aux autres utilisateurs de Cisco AMP Threat Grid.

Les « **Fichiers Privés** » sont des fichiers soumis à la solution AMP Threat Grid que vous choisissez de conserver à titre « Privé » afin qu'ils ne puissent être visualisés par d'autres utilisateurs de Cisco AMP Threat Grid.

« Poste(s) » désignent le nombre total d'utilisateurs autorisés à utiliser un service en nuage, selon le cas.

Les « **Données statistiques** » désignent toutes les informations et les données que Cisco déduit des données client, des données réseau ou des métadonnées de Cisco Cloudlock en sachant que ce type d'informations et de données est sous forme agrégée ou pour lesquelles les signes d'identification ont été retirés de sorte qu'il n'est pas raisonnablement possible de les utiliser pour identifier une personne ou votre entité.

*****

Annexe B

Définitions Cloudlock

Les définitions suivantes s'appliquent seulement pour Cisco Cloudlock et votre commande de Cisco Cloudlock et ont préséance en cas de contradiction avec le contrat ou avec **l'annexe A** de la description de cette offre :

La « Règle en vigueur » désigne une règle prédéfinie qui est fournie avec Cisco Cloudlock ou une règle que vous créez dans la mesure où une telle règle est affichée comme en vigueur dans Cisco Cloudlock.

Les « Métadonnées de Cisco Cloudlock» représentent l'information et les données générées ou recueillies dans l'utilisation de Cisco Cloudlock et stockées sur Cisco Cloudlock y compris, des renseignements sur l'utilisation du service en nuage couvert, comme les comptes utilisateur, les noms d'utilisateur, la structure organisationnelle (groupes, unités organisationnelles, etc.), autorisations (p. ex., Alice peut accéder aux fichiers dans le répertoire « pays des merveilles »); les Fichiers, les relevés et autres renseignements relatifs à des documents comme les titres, identifiants, tailles, types, et détenteurs des documents; dates d'enregistrement, de création ou de modification des fichiers; structure de dossiers; les renseignements relatifs aux connexions et déconnexions notamment les adresses IP et leur localisation; les informations relatives à l'accès aux documents (p. ex., Alice a téléchargé le fichier X à la date et à l'heure Y); les modifications de configuration apportées par les utilisateurs au service en nuage couvert ou à leurs comptes; les paramètres de configuration de Cisco Cloudlock; les paramètres de sécurité; les renseignements sur les applications tierces installées ou connectées au service en nuage couvert (p. ex., les identifiants, la date et l'heure d'installation, les autorisations et les activités); les règles (expressions courantes y comprises) mises en vigueur ou configurées par vous pour une utilisation de Cisco Cloudlock; les incidents et alertes signalés par Cisco Cloudlock; les journaux et fichiers d'audit; et les raccourcis et les jetons d'authentification qui vous ont été transmis pour permettre l'accès au service en nuage couvert visé.

Les « Services de base Cloudlock de Cisco » désignent, à compter de la date de lancement de cette description d'offre, ce qui suit : Cloudlock pour Google, Cloudlock pour Salesforce, Cloudlock pour Dropbox, Cloudlock pour Box, Cloudlock pour Microsoft Office365, Cloudlock pour ServiceNow et le connecteur d'application de Cloudlock pour Slack. D'autres services de base peuvent être offerts pour Cisco Cloudlock de temps à autre.

Les « Services en nuage couverts » désignent les logiciels-services correspondant aux environnements Saas, PaaS ou IaaS pour lesquels vous utiliserez Cisco Cloudlock (p. ex.,vos environnements Salesforce, Box ou Dropbox).

Les **« Ressources de données »** désignent un fichier discret unique, un enregistrement, un document ou tout autre objet relatif aux services en nuage couverts correspondants.

Le « Domaine » désigne une seule installation, une occurrence ou un domaine du service en nuage couvert. P. ex., un Domaine est une installation de Google Apps ou une installation ou compte Salesforce.

La **« Surveillance rétroactive »** désigne la capacité d'évaluer l'ensemble de vos données inactives en fonction des violations de règle notamment tous les objets historiques de données accessibles dans l'application du nuage.

Une **« Licence d'étudiant universitaire »** couvre un utilisateur qui est un étudiant d'un établissement d'enseignement supérieur. Les licences des étudiants poursuivant des études supérieures comprennent les cas d'utilisation de l'UEBA et les applications.

Les **« Licences d'élèves du secteur primaire et secondaire»** couvrent les utilisateurs qui poursuivent des études dans un établissement de niveau primaire et secondaire. Les licences des élèves du secteur primaire et secondaire comprennent les cas d'utilisation de DLP e des applications.

L'« Environnement d'essai et de mise au point » désigne un environnement sur Cisco Cloudlock où vous êtes autorisés à effectuer des essais et des mises au point pour le moindre de ces deux nombres : 1 000 utilisateurs au total ou le nombre de licences utilisateur achetées pour les principaux services de Cisco Cloudlock.

Les « Utilisateurs » désignent les utilisateurs individuels (actifs, interrompus ou autres) sur le service en nuage couvert correspondant contrôlé et analysé par Cisco Cloudlock.

*****